DATENBLATT

WATCHGUARD ADVANCED REPORTING TOOL

Verwertbare IT- und Sicherheitsinformationen

PROAKTIVE VERBESSERUNG DES SICHERHEITSSTATUS

Da Unternehmen immer mehr Sicherheitsdaten verwalten müssen, können sich die IT-Teams nicht mehr gebührend auf wichtige Details konzentrieren. Diese Daten können zur Erkennung von Sicherheitsproblemen und -verletzungen, die durch externe Faktoren und interne Mitarbeiter verursacht werden, genutzt werden.

Sicherheitsexperten sind durch das Datenvolumen überlastet. Die große Menge an verwalteten Daten und das Aufkommen von Malware der nächsten Generation führen dazu, dass viele Details übersehen oder nicht registriert werden, was die Sicherheit des gesamten Systems gefährdet.

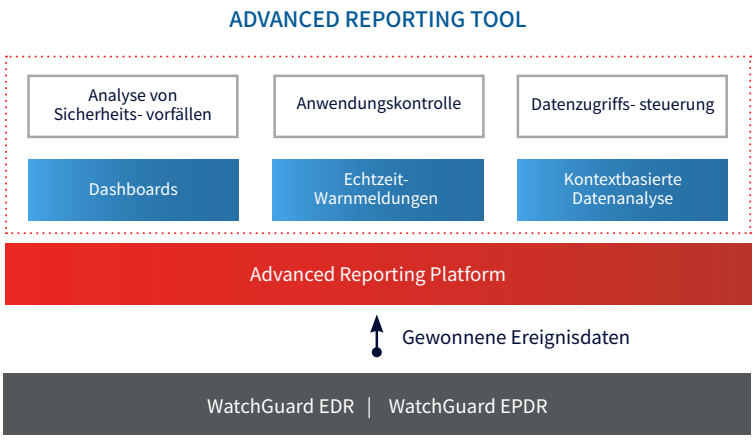
WATCHGUARD ADVANCED REPORTING TOOL

Die Advanced Reporting Tool (ART)-Plattform automatisiert die Speicherung und den Abgleich der von WatchGuard EDPR und WatchGuard EDR aus Endpoints gewonnenen Prozessdaten mitsamt Kontext, ohne dass Investitionen in Infrastruktur, Anlagen oder Wartung getätigt werden müssen.

Mithilfe dieser Daten kann das **WatchGuard Advanced Reporting Tool** automatisch Sicherheitsinformationen generieren und Tools bereitstellen, mit denen Unternehmen Angriffe und ungewöhnliche Verhaltensmuster unabhängig vom Entstehungsort präzise bestimmen sowie internen Missbrauch der Firmennetzwerke und -systeme erkennen können.

Mit dem **Advanced Reporting Tool** können Unternehmen Daten durchsuchen, untersuchen und analysieren. So werden IT- und Sicherheitseinblicke ermöglicht, darunter:

- Bestimmung des Ursprungs von Sicherheitsvorfällen, um zukünftige Angriffe zu verhindern
- Implementierung restriktiver Richtlinien für den Zugriff auf wichtige Unternehmensdaten
- Monitoring und Kontrolle des Missbrauchs von Unternehmensressourcen mit möglichen Auswirkungen auf die Unternehmens- und Mitarbeiterleistung
- Korrektur des Verhaltens von Mitarbeitern, sofern diese sich nicht an die Nutzungsrichtlinien des Unternehmens halten



HAUPTVORTEILE

Zugriff auf wichtige Informationen

- Maximieren Sie Ihren Einblick in alle auf den eingesetzten Geräten laufenden Prozesse und erhöhen Sie die Effizienz und Produktivität der IT-Abteilung.
- Greifen Sie auf Protokolldaten zu, um die Sicherheit der Unternehmensressourcen und Nutzungsindikatoren zu analysieren.
- Erhalten Sie detaillierte Informationen, um Sicherheitsrisiken sowie den Missbrauch der IT-Infrastruktur durch Insider zu identifizieren.

Diagnose von Netzwerkproblemen

- Gewinnen Sie Informationen über die Ressourcennutzung und die Verhaltensmuster von Anwendern. Nutzen Sie diese Informationen, um Anwender zu schulen und Richtlinien für Kosteneinsparungen zu implementieren.
- Erhalten Sie Einblicke in die im Netzwerk ausgeführten Computer und Anwendungen, um die Sicherheit und Kontrolle der Vermögenswerte Ihres Unternehmens zu verbessern.

Warnen und gewarnt werden

- Wandeln Sie entdeckte Anomalien in Echtzeit-Warnungen und Berichte um.
- Ermitteln Sie Sicherheitsabweichungen sowie den Missbrauch von IT-Ressourcen durch Mitarbeiter in Echtzeit.

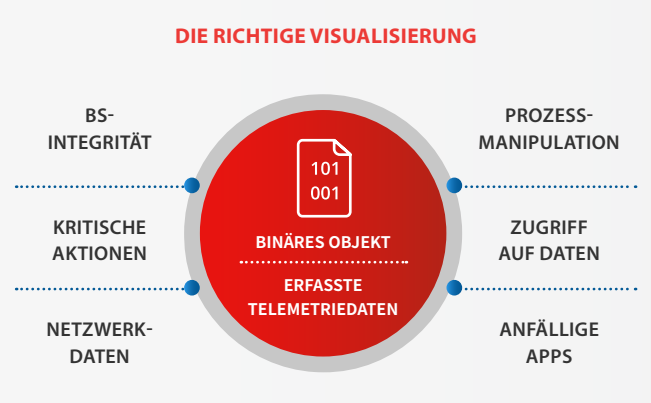
Auf Sicherheitsvorfälle vorbereitet sein

- Generieren Sie konfigurierbare Berichte, um methodische Analysen des Sicherheitsstatus Ihres Unternehmens durchzuführen, den Missbrauch von Vermögenswerten Ihres Unternehmens und Verhaltensanomalien festzustellen.
- Analysieren Sie den Status wichtiger Sicherheitsindikatoren und verfolgen Sie deren Entwicklung zur Evaluierung der eingeführten Korrekturmaßnahmen.

FLEXIBLE, AUF IHREN BEDARF ABGESTIMMTE ANALYSEN

Das **Advanced Reporting Tool** umfasst Dashboards mit Schlüsselindikatoren, Suchoptionen und Standardwarnmeldungen für drei zentrale Bereiche:

- Sicherheitsvorfälle
- 365-Tage-Speicherung für Daten
- Zugriff auf wichtige Informationen
- Nutzung von Anwendungen und Netzwerkressourcen
- Suchvorgänge und Warnmeldungen können dabei an die individuellen Gegebenheiten Ihres Unternehmens angepasst werden.



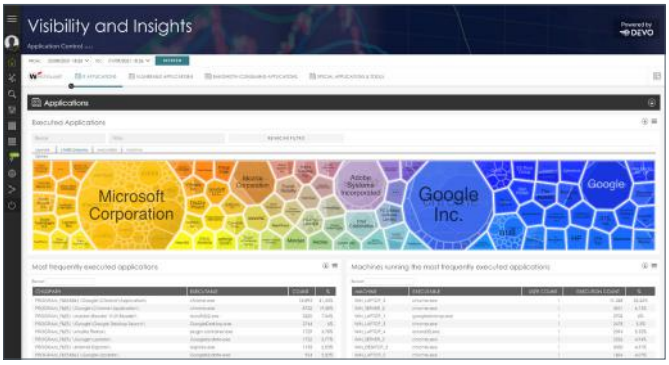
INFORMATIONEN ÜBER SICHERHEITSVORFÄLLE

Generieren Sie detaillierte Sicherheitsinformationen, indem Sie die während der Angriffsversuche aufgetretenen Ereignisse zeitnah verarbeiten und abgleichen:

- Zeitleisten mit Informationen zu Malware, PUPs und Exploits, die im vergangenen Jahr entdeckt wurden
- Computer mit den meisten Infektionsversuchen und entdeckten Malware-Exemplaren
- Computer mit gefährdeten Anwendungen
- Ausführungsstatus von Malware, PUPs und Exploits

SCHATTEN-IT-ERKENNUNG

- Am häufigsten und am seltensten ausgeführte Anwendungen
- Scripting-Anwendungen (PowerShell, Linux-Shell, Windows cmd usw.)
- Remote-Access-Anwendungen (TeamViewer, VNC usw.)
- Unerwünschte Freeware-Anwendungen (Emule, Torrent usw.)



MUSTER BEI DER NUTZUNG VON NETZWERKRESSOURCEN

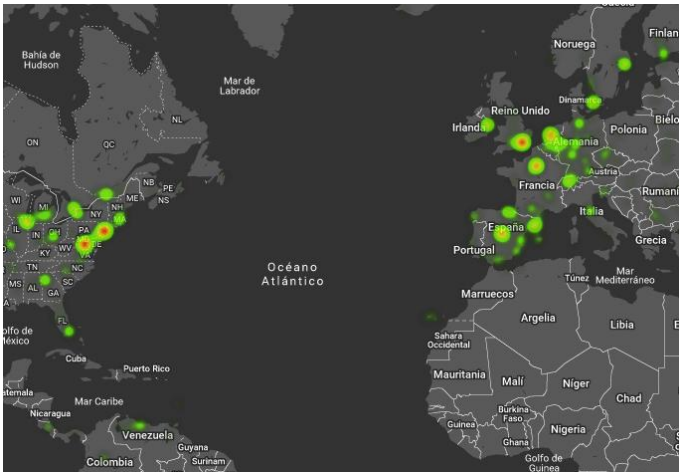
Erkennen Sie Muster bei der Nutzung von IT-Ressourcen, um Sicherheitsrichtlinien festzulegen und durchzusetzen:

- Feststellen, welche Unternehmensanwendungen und Nicht-Unternehmensanwendungen in Ihrem Netzwerk ausgeführt werden
- Anfällige Anwendungen, die im Netzwerk ausgeführt oder installiert werden und zu Infektionen führen oder sich auf die Unternehmensleistung auswirken können
- Steuerung der MS-Office-Lizenzen, Vergleich zwischen genutzten und erworbenen Lizenzen
- Anwendungen mit dem höchsten Bandbreitenverbrauch

KONTROLLE DES ZUGRIFFS AUF GESCHÄFTSDATEN

Zeigt den Zugriff auf vertrauliche Dateien im Netzwerk:

- Dateien, die am häufigsten von Netzwerkanwendern abgerufen und ausgeführt werden
- Zeitleisten und Karten mit Informationen zu den Daten, die im vergangenen Jahr gesendet wurden
- Identifizierung der Anwender, die auf bestimmte Computer im Netzwerk zugegriffen haben
- Länder, die die meisten Verbindungen von Ihrem Netzwerk empfangen



ECHTZEIT-WARNMELDUNGEN

Konfigurieren Sie Warnmeldungen für mögliche Sicherheitsverletzungen oder Verstöße gegen die Datenmanagementrichtlinie des Unternehmens:

- Standardwarnmeldungen zur Anzeige von Risikosituationen
- Unternehmensspezifische Warnmeldungen, die auf Anfragen von Anwendern basieren
- Sieben Methoden der Informationsdarstellung (mittels Bildschirmanzeige oder per E-Mail, JSON, Service Desk, Jira, Pushovery und PagerDuty)

Unterstützte Plattformen und Systemanforderungen von WatchGuard Advanced Reporting Tool

Kompatibel mit folgenden Lösungen: WatchGuard EDR, WatchGuard EPDR, und WatchGuard Advanced EPDR

Liste kompatibler Browser:
Google Chrome und Mozilla Firefox (weitere sind möglicherweise kompatibel).

Deutschland, Österreich, Schweiz +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de WatchGuard Technologies, Inc.